

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

IN THE MATTER OF THE SEARCH OF  
THE ORIGINAL EXTRACTION OF AN  
APPLE IPHONE 13 PRO MAX WITH  
SERIAL NUMBER CD690JYWVT,  
CURRENTLY LOCATED AT THE  
HICKORY POLICE DEPARTMENT, 347  
2<sup>ND</sup> AVE. SW, HICKORY, NC 28602

Case No. 3:25-mj-00077-WCM

**AFFIDAVIT IN SUPPORT OF AN**  
**APPLICATION UNDER RULE 41 FOR A**  
**WARRANT TO SEARCH AND SEIZE**

I, Jared Schaefer, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic extraction of a device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation Charlotte Division / Hickory Resident Agency and have been since October 2023. My career in law enforcement began in May 2020, where I spent three years as a sworn Police Officer/Detective with the La Porte Police Department (LPPD) in Indiana. I completed the police academy and performed road patrol duties, which consisted of responding to 911 calls for police assistance for all types of crimes, conducting self-initiated activities to deter crime, taking part in community engagement initiatives, and numerous other jobs vital to LPPD's mission. I then became a member of the Detective Bureau, where I conducted investigations into robberies, burglaries, sexual assaults, child molestations, murder, and other violent crimes for approximately two years. In my time as

a law enforcement officer, I have received several hundred hours of training in the investigations of general crimes, and I have been directly or indirectly involved with investigations of cases of child sexual assault. I have participated in the execution of numerous search warrants, which have resulted in the seizure of evidence and the successful prosecution of individuals.

3. For the purpose of supporting this Application for a Search Warrant, I have set forth herein facts that I believe are sufficient to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession of, knowing access, or attempted access with intent to view child pornography) by Tony SEE will be found in the extraction described below.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **IDENTIFICATION OF THE EXTRACTION TO BE EXAMINED**

5. The property to be searched is a forensic extraction of an Apple iPhone 13 Pro Max with serial number CD690JYWVT, hereinafter the “EXTRACTION.” The EXTRACTION is currently located at 347 2<sup>nd</sup> Ave SW, Hickory, North Carolina 28602 (Hickory Police Department).

6. The warrant would authorize the forensic examination of the EXTRACTION for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **BACKGROUND TO THE INVESTIGATION**

7. From March 2024 to December 2024, the Hickory Police Department (“HPD”) conducted six controlled purchases of illegal narcotics from SEE. To make these controlled purchases, HPD used a confidential informant (“HPD CI”) who had stated that the HPD CI had

previously bought marijuana and cocaine from SEE. The dates of the controlled purchases and the type and quantity of illegal narcotics that the HPD CI purchased from SEE are listed below:

- a. March 14, 2024, involving approximately 28.03 grams of cocaine;
- b. April 4, 2024, involving approximately 445.4 grams of methamphetamine;
- c. April 23, 2024, involving approximately 444.8 grams of methamphetamine;
- d. May 17, 2024, involving approximately 442.6 grams of methamphetamine;
- e. September 17, 2024, involving approximately 56.16 grams of cocaine; and
- f. December 6, 2024, pending results from DEA Laboratory.

8. During each controlled purchase listed above, law enforcement searched HPD CI prior to and after the controlled purchase. Other than the narcotics obtained during the controlled purchase, HPD CI did not have any narcotics. All controlled purchases were audio and video recorded. HPD CI was under constant surveillance of law enforcement prior to, during, and after the transactions of illegal narcotics in exchange for money.

9. All special funds used for the purchase of illegal narcotics were pre-recorded prior to each purchase in the event that the illicit funds were located inside the residence during the execution of the search warrant of SEE's residence, located at 450 13th Ave Ne, Hickory, North Carolina 28601 ("SEE Residence").

10. Each of the controlled purchases listed above were conducted at the SEE Residence. Accordingly, on December 10, 2024, HPD secured a search warrant for the SEE Residence.

11. On December 11, 2024, HPD executed the search warrant and seized multiple firearms, a ballistic vest, and trafficking amounts of narcotics.

12. During the course of the search, HPD also seized a gold Apple iPhone 13 Pro Max cell phone from SEE's person ("SEE's iPhone").

### *Extraction of See's iPhone*

13. On December 13, 2024, HPD secured a search warrant for SEE's iPhone. As described in the warrant, the crimes being investigated at that time were in relation to the North Carolina Controlled Substance Act 90-95. Additionally, the items to be seized described "evidence that may relate to this case, involving narcotics and firearms violations." The items to be seized further described "any and all stored digital content," including messages and attached multimedia files, such as pictures. In support of the warrant, the affidavit described the controlled purchases referenced above and noted that the HPD CI and SEE were "in constant communication . . . through text messages and also using the Snapchat application."

14. After obtaining the warrant for SEE's iPhone, a forensic analyst at HPD extracted the data from SEE's iPhone. The forensic extraction process used universal forensic extraction tools by connecting the target mobile device to the forensic hardware through a secure interface. The forensic tool then executed a systematic data acquisition protocol that bypassed the device lock, implemented write-blocking to prevent data modification, and created a verified copy of the device contents. The tool generated hash values to verify data integrity and produced standardized reports documenting the extracted information in accordance with forensic best practices. This process generated the EXTRACTION, the subject of this search warrant.

15. The EXTRACTION is a data set that cannot be read or reviewed by a human examiner without first parsing the data file utilizing digital forensics software. In other words, the EXTRACTION is a preserved copy of SEE's iPhone, but an examiner cannot view pictures, read files, etc., from the EXTRACTION without first converting the data set back into a usable form through the use of forensic software, such as Cellebrite, Axiom, and Griffey.

16. The EXTRACTION was preserved in Hickory Police Department's forensic laboratory, located at 347 2<sup>nd</sup> Avenue SW, Hickory, North Carolina 28602, per their standard practice and operating procedures. The EXTRACTION is in substantially the same state as it was when the EXTRACTION first came into the possession of the Hickory Police Department.

17. After creating the EXTRACTION, the HPD forensic analyst began searching the EXTRACTION for evidence of drugs and guns pursuant to the December 13, 2024, warrant. In reviewing the EXTRACTION, however, the forensic analyst observed thousands of media files in plain view, some coming from the Telegram Application, depicting child pornography, as defined in 18 U.S.C. § 2256(8) (referred to as Child Sexual Abuse Material or "CSAM"). Based on my training and experience, I know that the Telegram Application is a messaging platform that allows individuals to send messages and media to each other. Given the fact that the HPD forensic analyst saw CSAM media coming from the Telegram Application, this media was probably sent or received by the See iPhone in messages with other individuals using the Telegram Application. Upon seeing the CSAM, the forensic analyst stopped further review of the EXTRACTION pending the application of an additional search warrant that specifically included CSAM. The HPD forensic analyst is a Task Force Officer for the FBI. He has received training on child exploitation violations codified in 18 U.S.C. 2252A, including subsections (a)(2)(A) and (a)(5)(B) involving distribution, receipt, and possession of child pornography, as that term is defined in 18 U.S.C. 2256(8). The HPD forensic analyst has previously conducted many investigations and forensically analyzed thousands of devices that have been the source of evidence used for federal cases. Additionally, the forensic analyst has testified in the Western District of North Carolina as an expert regarding his forensic analysis of electronic devices and the evidence of child pornography contained therein.

18. On January 8, 2025, HPD obtained a search warrant to return to the SEE Residence to search for all electronics that could contain CSAM. HPD seized other devices from the See Residence, which are undergoing forensic analysis.

19. After obtaining the January 8, 2025, warrant for the SEE Residence, the forensic analyst continued searching the EXTRACTION and discovered more CSAM. While the observation of additional CSAM in SEE's iPhone was in plain view and can be lawfully seized,<sup>1</sup> the instant warrant application is not relying on any CSAM that the forensic analyst may have observed when he continued his search after the January 8, 2025, warrant for CSAM at the SEE Residence was obtained.

20. Your Affiant therefore requests this warrant to search the EXTRACTION, a preserved forensic copy of SEE's iPhone, for evidence of CSAM, as described in Attachment B.

### **TECHNICAL TERMS**

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Forensic extraction: A forensic extraction represents a comprehensive digital evidence collection process, which creates a duplicate of a mobile device's contents while maintaining forensic integrity. This procedure attempts to capture all data present on the device, including active user content, deleted information, system logs, and metadata, producing a forensically sound copy that preserves the evidentiary value of the digital content for potential legal proceedings.

---

<sup>1</sup> *United States v. Williams*, 592 F.3d 511, 522 (2010) (“any child pornography viewed on the computer or electronic media may be seized under the plain-view exception”).

- b. Processed data: Extracted data presented in a human readable format for review or investigation purposes.
- c. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

- e. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- f. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected



to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- g. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
22. Based on my training, experience, and research, I know that the EXTRACTION contains SEE's iPhone's capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on the extraction of the devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the iPhone.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools that create a forensic extraction.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the iPhone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the EXTRACTION because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on the extraction can also indicate who has used or controlled the iPhone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic iPhone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the EXTRACTION of the iPhone consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the extraction to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine an extraction already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**


27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the EXTRACTION described in Attachment A to seek the items described in Attachment B.

Respectfully,

/s/ Jared Schaefer  
Jared Schaefer  
Special Agent FBI

This affidavit was reviewed by AUSA Daniel Cervantes.

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 26th day of March, 2025, at 3:31 PM

  
W. Carleton Metcalf  
United States Magistrate Judge



## **ATTACHMENT A**

The property to be searched is a forensic extraction of an Apple iPhone 13 Pro Max with serial number CD690JYWVT, hereinafter the “EXTRACTION.” The EXTRACTION is currently located at 347 2nd Ave SW, Hickory, North Carolina 28602.

This warrant authorizes the forensic examination of the EXTRACTION for the purpose of identifying the electronically stored information described in Attachment B.

## **ATTACHMENT B**

All records and information in the EXTRACTION described in Attachment A that constitute evidence, contraband, or property designed for use, intended for use, or used in committing violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of, knowing access, or attempted access with intent to view child pornography) and involve Tony SEE, including:

1. Records and information relating to child pornography, as defined in 18 U.S.C. § 2256(8), as defined in 18 U.S.C. § 2256(8) (as defined in 18 U.S.C. § 2256(8) and used interchangeably with the term “child sexual abuse material” or “CSAM”);
2. Records and information relating to child erotica, defined as materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions;
3. Records and information relating to the communication with others about CSAM or child erotica, as described in paragraph 2 of Attachment B; and
4. Evidence of user attribution showing who used or owned the iPhone associated with the EXTRACTION identified in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.